Amendments to the Claims:

The following listing of claims replaces all prior listings of claims:

Listing of Claims:

The following listing of claims replaces prior listings.

1. (Currently Amended) An apparatus, comprising:

a determiner, comprising one or more programmable processing elements, configured to determine whether a message received at a first network has been through a security check by determining whether or not the message has been received with security at a first layer;

a forwarder, comprising the one or more programmable processing elements, configured to forward the message within the first network regardless of the result of the determination; and

a modifier, comprising the one or more programmable processing elements, configured to modify the message so as to include a second layer indication that the message has not been through [[a]] the security check applied at a security interface between two security domains ~~at the first layer~~ prior to being received at the first network when the result of the determination is that the message has not been through [[a]] the security check, wherein the second layer is a higher layer than the first layer;

wherein the forwarder is further configured to forward the message without modification in response to the determination being that the message has been through the security check applied at the security interface prior to being received at the first network.

2. (Previously Presented) The apparatus according to claim 1, further comprising:

a receiver configured to receive messages via a secure interface and a second network and directly from outside the first network.

3. (Cancelled)

4. (Previously Presented) The apparatus according to claim 1, wherein the message comprises a second layer identity header, and wherein the modifier is configured to include the second layer indication in the second layer identity header of the message.

5. (Previously Presented) The apparatus according to claim 4, wherein the message comprises a session initiation protocol message.

6. (Previously Presented) The apparatus according to claim 4, wherein the identity header comprises a p-asserted identity.

7. (Previously Presented) The apparatus according to claim 1, wherein the message comprises a second layer identity header, and wherein the modifier is further configured to modify the message so as to indicate that the message has not been through a security check by removing at least part of the second layer identity header.

8. (Previously Presented) The apparatus according to claim 7, further comprising:
a detector configured to detect whether the second layer identity header is of a particular type and when so to remove at least part of the header.

9. (Previously Presented) The apparatus according to claim 7, wherein the message comprises a session initiation protocol message.

10. (Previously Presented) The apparatus according to claim 8, wherein the detector is configured to detect whether the second layer identity header comprises a p-asserted identity.

11. (Cancelled)

12. (Cancelled)

13. (Previously Presented) The apparatus according to claim 1, wherein the apparatus comprises an interrogating call session control function.

14.-21. (Cancelled)

22. (Currently Amended) A system, comprising:

a security server comprising one or more programmable processing elements; and

a network processing element, comprising the one or more programmable processing elements, the security server being configured to receive a message, determine whether the message has been through a security check by determining whether or not the message has been received with security at a first layer, when the result of the determination is that the message has not been through [[a]] the security check applied at a security interface between two security domains modify the message so as to include a second layer indication that the message has not been through [[a]] the security check ~~at the first layer~~ applied at the security interface prior to being received at the security server, wherein the second layer is a higher layer than the first layer, and forward the message ~~to the network processing element~~ regardless of the result of the determination;

wherein the network processing element is configured to forward the message without modification in response to the determination being that the message has been through the security check applied at the security interface prior to being received at the first network.

23. (Previously Presented) The system according to claim 22, wherein the security server is configured to receive messages via a secure interface and another security domain and directly from outside the system.

24. (Previously Presented) The system according to claim 22, wherein the network processing element is configured to,

receive a message forwarded by the security server, and

determine whether the message has been modified so as to include a second layer indication that the message has not been through a security check, and, when the message has been so modified, perform one or more security checks in respect of the message.

25. (Currently Amended) A method, comprising:

determining that a message received at a first network has not been through a security check by determining that the message has not been received with security at a first layer;

modifying the message so as to include a second layer indication that the message has not been through [[a]] the security check applied at a security interface between two security domains ~~at the first layer~~ prior to being received at the first network, wherein the second layer is a higher layer than the first layer; and

forwarding the message within the first network;

wherein forwarding the message includes forwarding the message without modification in response to the determination being that the message has been through the security check applied at the security interface prior to being received at the first network.

26.-45. (Cancelled)

46. (Currently Amended) An apparatus, comprising:

determining means, comprising one or more programmable processing elements, for determining whether a message received at a first network has been through a security check by determining whether or not the message has been received with security at a first layer;

modifying means, comprising the one or more programmable processing elements, for, when the message is determined not to have been through [[a]] the security check, modifying the message to include a second layer indication that the message has not been through [[a]] the security check applied at a security interface

between two security domains ~~at the first layer~~ prior to being received at the first network, wherein the second layer is a higher layer than the first layer; and

forwarding means, comprising the one or more programmable processing elements, for forwarding the message within the telecommunications network regardless of whether the message has been through a security check;

wherein the forwarding means is further configured for forwarding the message without modification in response to the determination being that the message has been through the security check applied at the security interface prior to being received at the first network.

47.-55. (Cancelled)

56. (Previously Presented) The method according to claim 25, wherein the message comprises a second layer identity header, and comprising including the second layer indication in the second layer identity header of the message.

57. (Previously Presented) The method according to claim 56, wherein the message comprises a session initiation protocol message.

58. (Previously Presented) The method according to claim 56, wherein the identity header comprises a p-asserted identity.

59. (Previously Presented) The method according to claim 25, wherein the message comprises a second layer identity header, and further comprising:

modifying the message so as to include a second layer indication that the message has not been through a security check by removing at least part of the second layer identity header.

60. (Previously Presented) The method according to claim 25, further comprising:

detecting whether the second layer identity header is of a particular type and when so removing at least part of the header.

61. (Previously Presented) The method according to claim 60, wherein the message comprises a session initiation protocol message.

62. (Previously Presented) The method according to claim 61, further comprising:
detecting whether the second layer identity header comprises a p-asserted identity type.

63. (Cancelled)

64. (Currently Amended) The apparatus according to claim [[63]] 1, wherein the secure interface is a Za interface.

65. (Previously Presented) The apparatus according to claim 1, wherein the forwarder is configured to forward the message over a Zb interface.

66. (Cancelled)

67. (Currently Amended) The system according to claim [[66]] 22, wherein the secure interface is a Za interface.

68. (Previously Presented) The system according to claim 22, wherein the security server is configured to forward the message to the network processing element over a Zb interface.

69. (Cancelled).

70. (Currently Amended) The method according to claim [[69]] 25, wherein the secure interface is a Za interface.

71. (Previously Presented) The method according to claim 25, comprising forwarding the message within the first network over a Zb interface.